Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 November 2026

Vulnerabilities

CISA flags WordPress RCE flaw as actively exploited in attacks

BleepingComputer - 04 November 2026 08:11

The US Cybersecurity and Infrastructure Security Agency (CISA) warned federal agencies that attackers have started exploiting a recently patched high-severity WordPress vulnerability in the wild.

SonicWall warns of unpatched flaws in end-of-life GMS software

BleepingComputer - 04 November 2026 10:42

SonicWall warned customers of two security flaws affecting end-of-life Global Management System (GMS) systems that will not be patched.

CVE-2026-58868: Critical Android Bug Could Let Attackers Run Remote Code

Security Affairs - 04 November 2026 11:26

Critical Android flaw CVE-2026-58868 could allow remote code execution without user interaction on devices running Android 14 through 17.

Debian and Ubuntu APT Flaw Lets MitM Attackers Swap Verified Packages and Run Code as Root

The Hacker News - 04 November 2026 23:30

A flaw in APT, the package manager for Debian and Ubuntu, allows an attacker who can modify package downloads to swap a checked package for their own. The attacker's code then runs as root, according to advisories that Debian, Ubuntu, and APT's developers published on November 4.

Xen Hypervisor Flaws Let One Malicious VM Read and Write Any Other VM's Memory

The Hacker News - 04 November 2026 18:16

Two flaws in the Xen hypervisor allow a malicious guest virtual machine (VM) to read and write the memory of other VMs on the same host, including dom0.Dom0 is the VM that, by default, has full permissions and manages the others.

Scottish Cyber Coordination Centre

Google Issues Patches for Critical Android Flaw That Could Allow RCE Without User Interaction

The Hacker News - 04 November 2026 14:16

A critical Android flaw could allow an attacker to run code on a phone without any user action remotely, Google said in its November security bulletin.The flaw, CVE-2026-58868, affects Android 14 through 17. Phones get the fix with security patch level 2026-11-01 or later, which phone makers and carriers send on their own schedules.

Chrome 157 fixes 213 security issues, including 7 critical flaws

Malwarebytes - 04 November 2026 13:16

Your browser may not have updated itself yet. Here's how to check your version and install the fix manually.

Threat actors and malware

DreamHost confirms data breach exposed FTP logins and webmail sessions

BleepingComputer - 04 November 2026 15:05

DreamHost is warning of a data breach after attackers gained access to its File Manager platform for two months and stole customers' FTP/SFTP usernames and passwords.

mSecure password manager hack prompts password reset warnings

BleepingComputer - 04 November 2026 12:00

mSeven Software is warning current and former mSecure password manager customers to change passwords, reset two-factor authentication, and remove passkeys following a cyberattack that reportedly exposed an encrypted customer database.

Google Calendar phishing campaign hijacks sessions, bypasses MFA

BleepingComputer - 04 November 2026 11:00

A phishing campaign used Google Calendar invites, trusted redirects, and fake login pages to hijack corporate Google sessions and bypass MFA protections. Material Security examines how Operation CloudFire tracked the attacks, blocked malicious messages, and helped take down nearly 900 domains used by the attackers.

APT29-Linked Hackers Hijack Web Analytics Script to Deliver iOS and Android Exploits

The Hacker News - 04 November 2026 20:57

The Russia-linked threat actor known as APT29 is said to be behind a large-scale watering hole campaign targeting iOS and Android users through compromised websites, fake domains, and a supply chain attack involving a Ukrainian web analytics service called Plerdy SEO Tracker.

Scottish Cyber Coordination Centre

China-Aligned Group Abuses Sogou Input Method to Deliver Malware

Infosecurity Magazine - 04 November 2026 16:00

SlippyNunchucks used DNS hijacking to turn Sogou brand promotions into a malware channel